INFUSE HEALTH

HOW TO NAVIGATE AND MITIGATE THE RISKS OF HEALTHCARE CYBERATTACKS

IN 2024 AND BEYOND

INFUSE.com

The rise of cyberattacks in the healthcare sector has impacted patient care, data management, and overall business growth.

According to a 2023 study by Proofpoint, 88% of U.S. healthcare providers faced an **average of 40 cyberattacks during the year, and the average cost of a cyberattack was over $5 million, a 13% rise from the previous year.**

The healthcare sector is a key target for cybercriminals due to the value of patient data. Once stolen, this data is often sold on the dark web and used for phishing attacks, placing healthcare organizations, their staff, partners, and patients at risk.

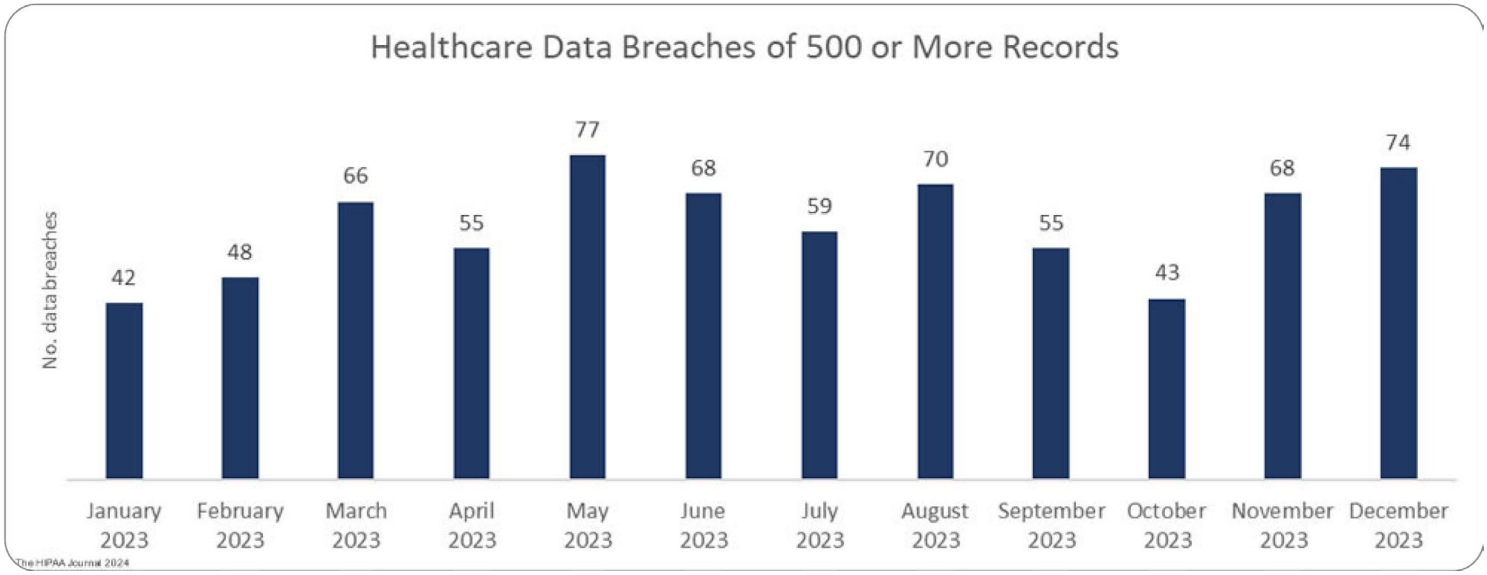
Addressing healthcare cyberattacks is imperative for maintaining patient trust and care. Security breaches compromise patient privacy and erode their confidence in healthcare providers. Implementing proactive measures, including robust cybersecurity protocols and fostering supply chain resilience, is paramount.

This article explores why cybersecurity is a critical part of effective healthcare and breaks down some of the biggest obstacles facing U.S. healthcare providers and strategies for overcoming them.

WHY TACKLING CYBERSECURITY IS THE TOP PRIORITY FOR HEALTHCARE PROVIDERS

The stringent regulations outlined by the Health Insurance Portability and Accountability Act (HIPAA) underscore the importance of safeguarding patient data. HIPAA mandates strict protocols for the protection of electronic health information and imposes significant penalties for non-compliance and negligence. In 2015, Anthem Inc. was fined $115 million for inadequate security controls after hackers stole the records of 79 million patients.

The Federal Trade Commission's (FTC) recent changes to the Health Breach Notification Rule (HBNR) also highlight the importance of effective healthcare cybersecurity. This new ruling requires personal health record (PHR) vendors not covered under HIPAA to notify individuals, the FTC, and occasionally the media in case of a breach—amplifying the potential impact of cyberattacks on brand reputation and acting as a catalyst for growth and shifts in the healthcare cybersecurity market.



Source: [The HIPAA Journal (2024)]

The financial, legal, and patient care impact of data theft compels healthcare providers to prioritize cybersecurity initiatives. According to a [2023 report by Compliancy Group], the cost of data theft per protected health information (PHI) record stands at over $180. To put this into perspective, **a mid-sized provider that reports a data theft of 100,000 PHI records would be fined $18 million.**

Mid- to large-size healthcare providers are delivering patient care in an increasingly digital landscape to efficiently deliver care. Yet, the rising dependence on digital care increases the probability of cyberattacks that threaten data security and patient outcomes.

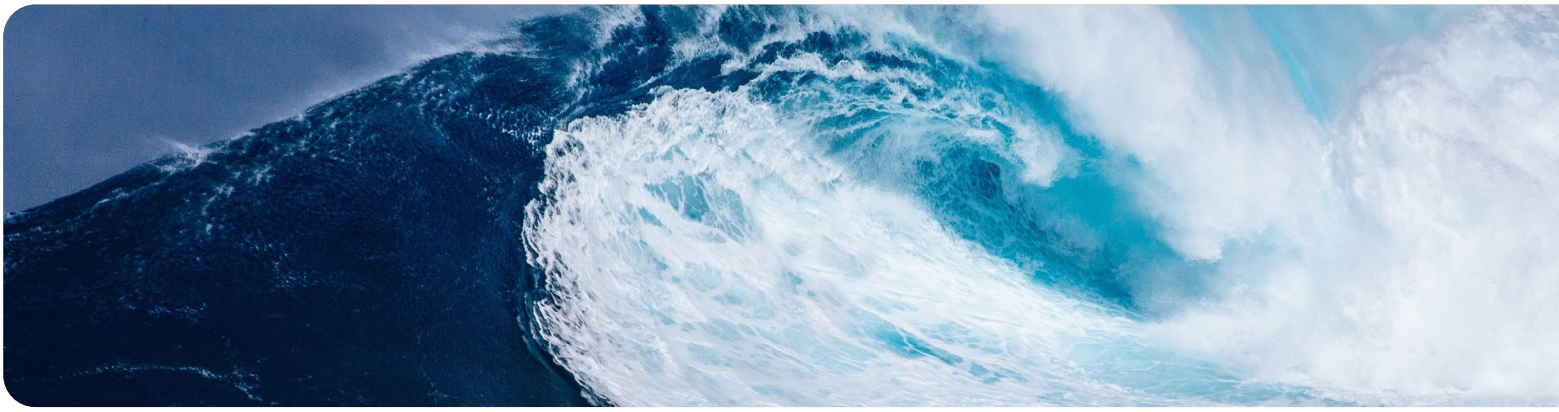
IMPACT OF CYBERATTACKS ON HEALTHCARE OUTCOMES

Healthcare professionals rely heavily on digital systems and electronic health records (EHRs) to access patient information, coordinate care, and make informed treatment decisions. However, in the aftermath of a cyberattack, these systems may become compromised or inaccessible, impeding the ability of care providers to deliver timely and effective treatments.

The impact of cyberattacks on healthcare providers and patients

Providers	Patients
Patient care disruption	Disruption in care provision
Financial impact, fines, and penalties	Sensitive information is compromised
Day-to-day operational challenges	Fear of personal cyberattacks due to data leaks
Inability to file claims	Inability to file claims
Cash flow challenges	Financial stress
Loss of patient trust	Lack of trust in the provider

The interruption of critical services, unauthorized access to medical devices, and manipulation of patient records can disrupt care, putting patient lives at risk. Cyber resilience measures are, therefore, essential to safeguard patient safety and prevent harm.



7 HEALTHCARE CYBERATTACKS TO WATCH FOR IN 2024 AND BEYOND

Below are seven common types of cyberattacks that healthcare organizations must take measures to prevent:

1. Phishing

Phishing is the most common cybersecurity threat in the healthcare sector and usually occurs via deceptive emails containing malicious links. These emails often cite familiar medical issues to encourage recipients to click on links. The more advanced phishing cyberattacks intercept ongoing patient-healthcare communications, making them seem more authentic.

When recipients click on phishing links, they are led to fake web pages that mimic login screens, where credentials are then harvested and used by cybercriminals to access healthcare systems.

Given its prevalence and financial impact, anti-phishing measures are a crucial element of healthcare cybersecurity strategies. This includes training for both staff and patients, including proactively communicating common scams to patients and how to avoid them (such as, for example, instating a protocol to never send out links to patients via SMS).

2. Data breach

The U.S. healthcare industry experiences a disproportionately high rate of data breaches, averaging 1.76 breaches per day. Despite stringent regulations mandating the protection of health records, many healthcare facilities struggle to implement effective security controls.

To mitigate these risks, healthcare institutions need to invest in attack surface monitoring solutions and enhance the security awareness of their third-party vendors to prevent data loss.

3. Ransomware

Healthcare institutions are prime targets for ransomware attacks. These attacks typically employ a virus delivered via malicious links or files. These encrypt data on infected computers, after which hackers demand a ransom to decrypt it. Due to the complexity of these viruses, prevention is crucial, as typically only the creators can decrypt them successfully.

Below are five best practices to prevent and mitigate the impact of ransomware attacks:

- **Maintain backups:** Data backup is crucial for ransomware recovery. Ensure backups are protected and stored offline. Cloud services aid recovery by retaining file versions. Regularly test backups for effectiveness and verify their integrity post-attack.
- **Plans and policies:** Develop a ransomware incident response plan with defined roles and communication procedures. Include contact lists for partners/vendors.
- **Review port settings:** Ransomware often targets RDP port 3389 and SMB port 445. Assess the necessity of leaving them open and restricting them to trusted hosts. Review settings for on-premises and cloud, and disable unused RDP ports with the provider's assistance.
- **Educate teams:** Cybersecurity training is vital for building awareness. Train team members to identify and avoid malicious emails by discerning suspicious elements in emails such as links and attachments. This ensures the collective defense of the organization against cyber threats.
- **Implement an Intrusion Detection System (IDS):** An IDS scans network traffic logs for known malicious activity using signatures. Regular signature updates and swift alerts enhance the ability to detect potential threats effectively.

4. DDoS attacks

Distributed Denial of Service (DDoS) attacks involve overwhelming a server with excessive requests, often crashing it. As a result, they can be devastating for crucial hospital systems given the catastrophic consequences that even an hour of downtime can have.

Attackers often demand a ransom to cease the attack. Unlike other cyber threats, where user vigilance is crucial, defending against DDoS attacks relies on IT departments adequately preparing. These include implementing robust technological measures, such as extra bandwidth, Content Delivery Network (CDN) services to filter malicious requests, and equipping servers with specific hardware protections.

5. Internal threats

Hospitals and clinics face significant risks in terms of data management with their staff or partners, with unintended confidential data leaks (or even intentional sabotage by ill-intended parties).

Establishing authorization protocols and a data access hierarchy is paramount, as well as anonymizing patient data whenever possible and utilizing Data Loss Prevention (DLP) tools to alert IT teams of unusual behavior.

6. Securing IoT devices

The Internet of Things (IoT) comprises interconnected devices, including health monitors and surgical robots. Despite the benefits of enhancing patient care, this connectivity also exposes the sector to cybersecurity threats such as ransomware, data breaches, and DDoS attacks.

Healthcare entities must regularly update IoT devices with the latest security patches, enforce strong authentication protocols, and use network segmentation to prevent the spread of attacks throughout their IoT infrastructure.

7. Supply chain risks

Attackers targeting healthcare systems often exploit vulnerabilities in supply chain weak points or third-party vendors. With the increased use of cloud services for storing patient records, cybersecurity risks have intensified. A study published by PR Newswire revealed that over 50% of healthcare IT respondents experienced a data breach within their cloud systems in 2023.

Common breaches occur due to inadequate cybersecurity practices or a lack of cybersecurity training among vendors. To enhance security, healthcare organizations should practice good cloud security hygiene, thoroughly understand their cloud services, and ensure that third-party providers adhere to robust security protocols.

To provide data security and uninterrupted patient care, healthcare providers need to build an ecosystem of cybersecurity around their networks.

This ecosystem rests on three pillars:

1. Implementing change management
2. Leveraging cybersecurity technologies and tools
3. Managing building access control with zero trust

HOW TO MITIGATE CYBERSECURITY RISKS: TOP 3 STRATEGIES

Below are the top three strategies you should implement to mitigate cyberattack risks:

Implement change management

Actioning internal change management involves instilling cybersecurity awareness, establishing protocols to respond to cyberattacks, and training healthcare teams.

To support cybersecurity awareness, healthcare institutions must foster a culture where every team member understands their role in protecting sensitive data. This includes conducting regular awareness campaigns and tests, emphasizing the importance of adhering to security protocols, and encouraging a proactive stance toward identifying and reporting potential threats.

Healthcare organizations should develop comprehensive incident response plans that outline step-by-step guidelines for detecting, assessing, and mitigating cyber threats. According to a 2022 study conducted by ASPR in conjunction with the U.S. Department of Health and Human Services (HHS), the defined protocols **should cover responses for eleven situations that arise from cyberattacks, including:**

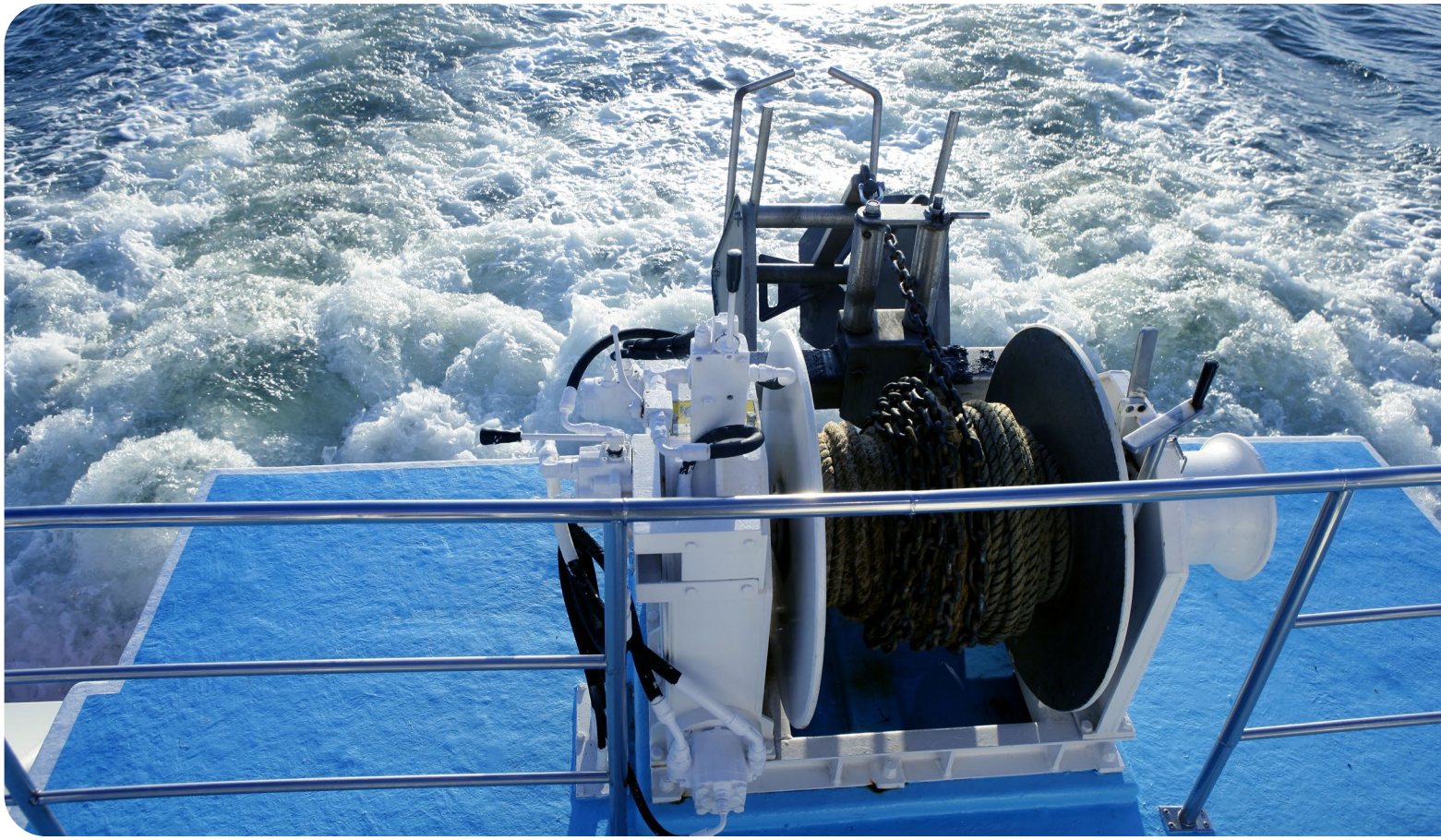
1. **Incident command principles**
2. **Workforce resilience**
3. **Response downtime procedures**
4. **Downtime forms**
5. **Operational considerations**
6. **Personnel adjustments**
7. **Safety considerations**
8. **System shutdown triggers**
9. **Response downtime procedures**
10. **Maintaining clinical practices**
11. **Communication and information sharing**

2. Leverage technology and digital security tools

Generative AI (genAI) tools are significant assets for automating threat detection and response. By harnessing the power of artificial intelligence (AI) and machine learning algorithms, healthcare organizations can augment their ability to detect anomalies and identify security breaches in real-time.

Below are the top five benefits of integrating genAI into your cybersecurity strategy:

1. **Adaptive threat detection**
2. **Predictive analysis**
3. **Enhanced biometrics for access**
4. **Automated security patch generation**
5. **Phishing detection and prevention**



3. Building access control in healthcare networks (zero trust)

Each user accessing healthcare networks does so with a unique identity, which is a combination of a username and password. As cyberattacks often start with a compromised identity, it is critical to define access limits for each identity based on their role (to minimize potential damage). Healthcare providers can achieve this by implementing zero trust.

The zero-trust security model is based on the distrust of all devices and users, requiring stringent controls for network access and segmentation. Both network and security teams collaborate to establish secure network perimeters and implement controls across LAN, WLAN, WAN, and remote access. This enables granular management of application and data access, thereby preventing and minimizing the impact of cyberattacks.

Below is a simplified process of how to implement zero trust across your healthcare network:

1. **Identify all users and devices:** Initiating a zero-trust network entails authenticating network connections. This can be facilitated with identity and access management tools to authenticate users and devices. Simplicity and consistency in this process for end users across various connections is imperative for effective cybersecurity.

2. **Implement access control and micro-segmentation:** Zero-trust frameworks limit application and service access (via microsegmentation) to only the most essential requirements post-identification. Next-gen firewalls, common for microsegmentation, also provide precise access policy creation for network applications.

3. **Establish continuous monitoring and alerting processes:** Monitoring device behavior is essential in a zero-trust network. Utilizing tools like network detection and response or AIOps platforms enables real-time tracking of communication patterns, identifying and prioritizing potential threats.

4. **Consider remote access:** Legacy remote access VPNs are inadequate for modern corporate networks due to inefficiency and excessive network access. Suppliers now offer new methods aligned with zero-trust principles, improving authentication, microsegmentation, enhanced visibility, and centralized access control for both on-premise and cloud environments.

KEY TAKEAWAYS

Keep in mind the following takeaways to ensure the cybersecurity of your healthcare organization:

- Healthcare cyberattacks impact patient care, have a significant financial impact on providers, and lead to a loss of patient trust and reputation. HIPAA levies heavy penalties in cases where the provider has not provided adequate data security
- Healthcare providers must build a robust security framework that includes implementing change management, leveraging AI and security technology and tools, and implementing access control with zero trust
- Working with trusted external partners, including demand generation providers, helps healthcare providers develop security frameworks and secure brand reputation

HOW INFUSE HEALTH CAN HELP HEALTHCARE PROVIDERS NAVIGATE CYBERSECURITY

INFUSE Health experts understand the significant cybersecurity threats facing healthcare providers, and their implications.

By delivering tailor-made demand generation programs, **INFUSE Health empowers healthcare organizations** to build brand equity and cement cybersecurity resilience with patients and key partners.

Learn more about how INFUSE Health can drive your outcomes ⟶

DISCOVER MORE INFUSE INSIGHTS

Tackle Obstacles

5 Biggest Challenges for Healthcare Providers

→

Get Started With Demand Generation

How to Kickstart Your Demand Generation Strategy for Success

→

Discover The Latest Insights Into B2b Buyer Behavior

INFUSE Insights Voice of the Buyer 2024 Report

→

INFUSE

2385 NW Executive Center Drive, Suite 100
Boca Raton, FL 33431
info@infuse.com